Standardized E-Gas monitoring concept for engine management systems of gasoline and diesel engines

Version 4.0

1 GENERAL PART 4

1.1 Participants of the work group 4

2 INTRODUCTION 5

3 DEFINITIONS OF TERMS 6

4 ABBREVIATIONS 8

5 DEVELOPMENT GUIDELINES AND PRINCIPLES 9

6 TECHNICAL CONVERSION 11

6.1 The monitoring concept at three levels 11

6.1.1 System overview 11
6.1.2 Engine management functions and component monitoring of level 1 12
6.1.2.1 Characteristics and monitoring of the throttle-valve actuator 13
6.1.2.1.1 Characteristics of the throttle-valve sensor technology 13
6.1.2.1.2 Error detection 13
6.1.2.2 Version characteristics and monitoring of the pedal travel sensor 14
6.1.2.2.1 Version characteristics of the pedal travel sensors 14
6.1.2.2.2 Version characteristics of the control unit input circuits 14
6.1.2.2.3 Error detection 14
6.1.2.3 Determination of the pedal travel demand in level 1 in normal operation 15
6.1.2.4 Gas / brake plausibility 15
6.1.3 Level 2 function monitoring, general requirements 15
6.1.3.1 Inclusion torque loss from level 1 for the calculation of “permissible torque” 18
6.1.3.2 Transfer of adaptation values / correction factors from level 1 to level 2 (tolerance restriction) 18
6.1.3.3 Monitoring of the injection output variables from level 1 18
6.1.3.4 Monitoring of the trigger output unit (e.g. TPU, PCP) 18
6.1.3.5 Continuous torque monitoring diesel (torque comparison), determination actual torque level 2 19
6.1.3.5.1 Rail pressure monitoring 19
6.1.3.5.2 Torque relevant efficiencies of injection quantities 21
6.1.3.5.3 Further torque relevant efficiencies (e.g. air influence) 21
6.1.3.6 Continuous monitoring diesel (acceleration comparison) 21

6.1.3.6.1 Requirements level 1 21
6.1.3.6.2 Requirements level 2 22
6.1.3.7 Continuous torque monitoring diesel, overrun monitoring 22
6.1.4 Safeguarding of torque output variables in the control unit group 22
6.1.5 Level 3 controller monitoring 23
6.1.5.1 Monitoring of the question / answer communication 24
6.1.5.1.1 Monitoring via the L3_MM 24
6.1.5.1.2 Monitoring via the L3_SW in the function controller 24
6.1.5.2 Iteration rate of the question / answer communication 25
6.1.5.3 Test paths of the L3_SW in the function controller 25
6.1.5.4 Question generation in monitoring module L3_MM 25
6.1.5.5 TPU monitoring 26
6.1.5.6 Shutoff path test 27
6.1.5.7 A/D conversion test 27
6.1.5.8 System behavior at reset 28
6.1.5.9 Diagram of the level 3 error reactions 28
6.2 System reactions in case of error 29
6.3 Additional technical requirements 29
6.3.1 Safe engine stop 29
7 7 APPENDIX: ILLUSTRATIONS 30
8 APPENDIX : FAILURE REACTIONS 39
8.1 Error from the level 1 monitoring 39
8.1.1 Pedal-travel sensor 39
8.1.2 Throttle actuator (gasoline with one throttle-valve actuator) 40
8.1.3 Monitoring of external requests 40
8.1.4 Monitoring programming and supply voltage 41
8.1.5 Brake information 41
8.2 Failure from the level 2 functional monitoring 41
8.3 Failure from the level 3 controller monitoring 43

1 GENERAL PART

1.1 Participants of the work group

Company	Repres.	Dept.	Phone	Fax	e-mail
Audi AG	Nägler	I/EA-823	0841/89-90693	0841/8984-90693	heinrich.naegler@audi.de
BMW AG	Ertl	ZM-E-32	+43-7252/888-2298	+43-7252/888-62298	christian.ec.ertl@bmw.co.at
	Dr. Albrecht	EA-243	089/382-39160	089/382-32175	marc.albrecht@bmw.de
DC AG	Rehm	EP/MEI	07031/90-62744	07031/90-62774	lothar.rehm@daimlerchrysler.com
	Roth	EP/MAD	0711/17-58959	0711/30521 17996	herbert.roth@daimlerchrysler.com
Porsche AG	Staib	EEA2	0711/911-83545	0711/911-84858	thomas.staib@porsche.de
VW AG	Veldten	EAEF/2	05361/93-5480	05361/93-2839	burkhard.veldten@volkswagen.de

The work group EGAS thanks Mr. Schultalbers (IAV) and Mr. Pitzal (Bosch) for supporting the concept development of the enhanced monitoring systems of diesel engines.

2 INTRODUCTION

To control gasoline and diesel engines, „drive by wire“ systems are now state-of-the-art technology. The high requirements for these systems and their integration in networked vehicle systems mean that their functional capacities must be closely monitored.

The automotive manufacturers represented in the EGAS work group see no potential of brand-name differentiation in solving this mission. For this reason, they have agreed to standardize the monitoring concept for EGAS systems and to transpose this concept into the engine management systems on their vehicles, regardless of the supplier.

Despite functional differences for the engine management of gasoline and diesel engines which mainly concern different working procedures, the EGAS work group considers that it is possible to standardize monitoring core components and functions.

The available documentation describes the principles of the concept that must be used. It is intended to be used as a guide for the development of future engine management systems.

The EGAS monitoring concept used in the present document has been developed by the supplier comprehensive EGAS work group in collaboration with control unit manufacturers. The work group results are based on a basic concept that comes from Robert Bosch GmbH.

The document version on hand includes the description of a process of continuous torque monitoring of diesel engines in addition to the established overrun monitoring.

In addition to version 3.0, in the version on hand an alternative monitoring process for diesel engines is described, basing on a target-actual comparison of wheel-/ vehicle-acceleration quantity. This process is released by the EGAS work group as an equivalent process. The results of the work group are based on a VW/IAV concept.

When using this specification, the mutual license rights shall be cleared by the concerned legal and patent departments.

3 DEFINITIONS OF TERMS

- A **driving cycle** is the operation time between the engine start and stopping, including a control unit's power down phase.

- An **error** or **an individual error** is a failure to meet at least one requirement regarding a required characteristic of the considered unit.

- A **latent error** is an error that cannot be recognized in the next driving cycle either by the electronic engine management system or by the driver.

- **Double errors** are two errors that occur within a short period („simultaneous“) and that do not have any causal connection.

- Two individual errors that occur outside a short period and that do not have any causal connection are **dual errors.**

- **Error detection** : when authorized deviations for relevant system variables are exceeded, it causes at least one requirement that cannot be fulfilled for a relevant characteristic of the considered unit. An **error** is considered as **recognized** when the discovery time is sufficient to invert or reduce the error effect (serious).

- **The error effect** is a modification in system behavior in standard mode relative to system behavior in failure mode (the requirements of the concerned system parameters must be satisfied).

- **The consequence of the error** is all the measures that are introduced after an error has been detected in order to limit the consequences of the error to the authorized deviations.

- **Controllable system reactions** in the case of an error are characterized as follows:
  - defined approved reaction times
  - defined approved engine torque- /engine speed- or acceleration limits

- „**Raw signals**“ on the control unit are :
  - digital or analog input signals that are scanned in the input hardware registers
  - input information received via data bus that is taken-over as it is

- **Reset** refers to setting the systems in a controlled state.
  This can be triggered by means of a SW function call or a HW mechanism in the control unit :

  - SW reset: initiated by means of a function call (ROM-, RAM test , etc.)
  - HW reset: initiated by means of hardware measures (watchdog, power-on reset, etc.)

- The **safety fuel cut-off** limits maximum authorized engine rotational speed (for example via fade-out of torque relevant injections).

- The **pedal travel sensor** monitors the position of the accelerator pedal and therefore the driver's intention.

- The **timing processing unit** (TPU) or comparable co/sub-processors use time or angle synchronous inputs and/or outputs, which are relevant for the torque acquisition or torque conversion (for example, speed acquisition, driving the injection or ignition stages).

4 ABBREVIATIONS

Abbr. in G.	German	English	Abbr. in E.
ADC	Analog Digital Konverter	Analog Digital Converter	ADC
ARD	Aktiver Ruckeldämpfer	Active Jerk Damper	AJD
ASIC	Application Specific Integrated Circuit	Application Specific Integrated Circuit	ASIC
BLS	Bremslichtschalter	Stop Switch	SS
BTS	Bremstestschalter	Brake Test Switch	BTS
CAN	Controller Area Network	Controller Area Network	CAN
CR	Common Rail	Common Rail	CR
DEW	Drosselklappenersatzwert	Throttle Valve Default Value	TVDV
DK	Drosselklappe	Throttle Valve	TV
DK1	Drosselklappenwinkel aus Istwert1	Throttle Valve Angle from Actual Value 1	TV1
DK2	Drosselklappenwinkel aus Istwert2	Throttle Valve Angle from Actual Value 2	TV2
E3_SW	E3-Überwachungs-Software im Funktionsrechner	Level 3 Monitoring Software in the Function Controller	L3_SW
E3_ÜM	Ebene 3 Überwachungsmodul	Level 3 Monitoring Module	L3_MM
FGR	Fahrgeschwindigkeitsregelung	Cruise Control	CC
FMEA	Failure mode & Effect Analysis	Failure mode & Effect Analysis	FMEA
FR	Funktionsrechner	Function Controller	FC
HW	Hardware	Hardware	HW
IW	Istwert	Actual Value	AV
LL	Leerlauf	Idle	ID
MSR	Motor-Schleppmomenten-Regelung	Engine Drag Torque Control	MSR
n_mot	Motordrehzahl	Engine Speed	n_mot
PAK	Programmablaufkontrolle	Program Flow Checks	PFC
PWG	Pedalwertgeber	Pedal Travel Sensor	PTS
SG	Steuergerät	Control unit	CU
SRC	Signal range check	Signal range check	SRC
EMB	Einspritz-Mengen-Begrenzung	Injection Reduction	IR
SW	Software	Software	SW
TPU	Timing processing unit bzw. vergleichbare Co/Subprozessoren wie PCP	Timing processing unit or comparable co/subprocessor like PCP	TPU
ÜM	Überwachungsmodul	Monitoring Module	MM

5 DEVELOPMENT GUIDELINES AND PRINCIPLES

- Protection of life has the highest priority
- Reliability takes precedence over replacement functions
- The monitoring is to take place continuously independent of the engine concept and largely independent of driver reaction.
- Functions, especially those for system monitoring (error reaction included), must be clear and simple.
- The system concept must enable individual errors and individual errors in connection with latent errors to lead to controllable system reactions. The corresponding signal paths (sensors, actuators, functions) shall be monitored.
- The system concept must enable double / dual errors to lead to controllable system reactions as far as it is technically possible at the time of system definition.
- For possible high availability purposes, graduated error reactions shall be targeted.
- A signal path shall be only graduated after clear recognition (for example after debouncing event or time) as a „confirmed defect“, before the reaction mechanisms are activated. Previously the defect shall be graduated as „presumed defect“
- An appropriate reaction mechanism shall be defined according to the function and in case of a "presumed defect" or „confirmed defect“.
- The withdrawal of error reactions shall be determined in isolated cases and shall be carried out in a controlled manner. Unstable junctions shall be avoided.
- Engine stop is authorized when no other controlled system reaction can be provided.
- The transmitter is responsible for the content of its initiated messages on the control unit interface. This means that, for example, external torque requests must be guaranteed by the transmitting control unit. The transmission track and the up-to-dateness of the messages shall be checked by the engine management system.

- For errors that can lead to unwanted system reactions when related to subsequent errors, the driver should be informed (optically or by modifying driving behavior).

- Function controller monitoring must be kept stable and simple so it can be achieved with an ASIC.

- The efficiency of the redundant shutoff paths shall be tested in each driving cycle.

- Shutoff paths of the monitoring concept must be stable in case of defective power supply drifts and the power supply concept must be monitored to avoid possible damage to components. Controllable error reactions must be inserted.

6 TECHNICAL CONVERSION

6.1 The monitoring concept at three levels

6.1.1 System overview

The monitoring occurs at three levels:

Level 1

This is described as a **functional level**. It contains engine management functions, for example, to convert requested engine torque, component monitoring, input / output variable diagnostic and to control the system reactions when an error is discovered.

Level 2

This is described as **a function monitoring leve**l. It recognizes the defective sequence of level 1 functional software, for example, by monitoring the calculated torque values or the vehicle acceleration. In case of error, system reactions are triggered.

Level 3

This is described as **a controller monitoring leve**l. It contains a monitoring module that is independent of the function controller (for example ASIC or controller), which tests that the program has been correctly executed by means of a question-answer process. In case of error, system reactions are triggered independently of the function controller.

Illustration 1 in appendix

6.1.2 Engine management functions and component monitoring of level 1

Level 1 consists of:

- all engine management functions
- the diagnostic input and output variables related to monitoring

The following tables consider only present components that are relevant for the monitoring and dependent on the system. They are directly monitored or monitored according to the state-of-the-art technology (physical efficiency paths)

Sensor component	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Pedal travel sensor	x	x	x	x
Brake switch	x	x	x	x
Speed signal	x	x	x	x
Load signal	x	x		
Oxygen captor		x		
Common rail pressure sensor		x	x	
Engine temperature sensor	x	x	x	

Actuator component	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Throttle valve[1])	x	x		
Fuel injection cut-off	x	x	x	x
Common rail pressure valve			x [3)]	x [3)]
Metering unit			x [4)]	x [4)]

Signals from other control units	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Received requests that increase torque (signal transmission and up-to-dateness) [2)]	x	x	x	x
Vehicle acceleration (if applicable from vehicle speed)				x

Protected shutoff paths of the cruise control	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Brake information	x	x	x	x

[1]) if decisive for the air path
[2]) torque-increasing requests shall be guaranteed by the sending control unit
[3]) for CR systems with two actuator concept only
[4]) for CR systems only

6.1.2.1 Characteristics and monitoring of the throttle-valve actuator

6.1.2.1.1 Characteristics of the throttle-valve sensor technology

- Double sensor with physically separated signal paths
- High monitoring sensitivity over the entire adjustment range. Current standard is a version with performance curve progression in the opposite direction and the same voltage range.
- High resolution for good control accuracy and diagnostic
- Minor synchronism deviation for effective diagnostic
- Minor drift in environmental and durability conditions (maintain diagnostic limits)

6.1.2.1.2 Error detection

- Short-circuits, parallel connections and open-circuit on the throttle valve sensors (including sensor power supply)
- Short-circuits and open-circuits on the throttle valve drive.

Error	Possible error detection
Possible offset voltage supply or sensor mass	Signal-range-check or synchronism monitoring sensor 1 to sensor 2
Possible offset sensor 1 or sensor 2	Signal-range-check or synchronism monitoring sensor 1 to sensor 2
Short-circuit sensor 1 to sensor 2	Position monitoring (target/actual value or position adjust. monitor. (input variable)
Error at the actuator	Position monitoring (target/actual value or position adjust. monitor. (input variable)

6.1.2.2 Version characteristics and monitoring of the pedal travel sensor

6.1.2.2.1 Version characteristics of the pedal travel sensors

- Double sensor with physically separated signal paths
- Monitored sensor supply voltage or two sensor supply voltages
- Two electrically isolated sensor grounds
- Clear plausibility over the entire adjustment range. Current standard is a version with variable-slope increasing performances curves.
- Minor synchronism deviation and sufficient resolution for effective diagnostic
- Minor drift on environmental and durability conditions (maintain diagnostic limits, short pedal dead stroke)

6.1.2.2.2 Version characteristics of the control unit input circuits

- The sensor input circuits shall be determined so that a voltage level < idle arises in case of line open-circuit.

6.1.2.2.3 Error detection

- Short-circuits, parallel connections and open-circuits on the driving pedal travel sensors (sensor power supply included)

Error	Possible error detection
Potential offset of the voltage supply	Synchronism monitoring sensor 1 to sensor2 or reverse reading of the sensor supply voltage
Potential offset sensor 1 or sensor 2	Signal-range-check or synchronism monitoring sensor 1 to sensor 2
Short-circuit sensor 1 to sensor 2	Synchronism monitoring sensor 1 to sensor 2 or signal-range-check
Potential offset sensor ground 1 or Sensor ground 2	Synchronism monitoring sensor 1 to sensor 2 or signal-range-check

6.1.2.3 Determination of the pedal travel demand in level 1 in normal operation

The characteristic curve of sensor channel 2 initially is converted to the characteristic curve of sensor 1.
The calculation of the pedal travel demand in level 1 in normal operation is then carried out by a minimum selection of the two sensor channels.

6.1.2.4 Gas / brake plausibility

If it is detected that the driver actuates the brakes for an applicable time that exceeds an applicable vehicle speed threshold and for a driver "idle speed threshold" demand, the engine torque must be reduced to an applicable value.

6.1.3 Level 2 function monitoring, general requirements

The level 2 (function controller component) contains :

- monitoring of functions that determine level 1 performance

Central element of level 2 for systems with torque monitoring is the torque comparison between self-sufficient formed calculation variables of “permissible torque” and “actual torque”.
Central element of level 2 for systems with acceleration monitoring is the acceleration comparison between self-sufficient formed “permissible vehicle acceleration” and “actual vehicle acceleration”

- monitoring of level 1 error reaction if L2 cannot autonomously generate an error reaction.
- Level 2 storage areas that can be monitored cyclically
- arithmetic operations for program flow checking

A graphical representation can be found for:

- gasoline manifold injector in illustration 2 in appendix
- gasoline direct injector in illustration 3 in appendix
- diesel (torque comparison) in illustration 4 and illustration 5a in appendix
- diesel (acceleration comp.) in illustration 4 and illustration 5b in appendix

The following tables show the detailed monitoring tasks for level 2:

Signals from other control units	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Content of the transmitted monitoring relevant ranges	x [1)]	x [1)]	x [1)]	x [1)]
Vehicle acceleration, if applicable from vehicle speed (up-to-dateness + signal transmission)	-	-	-	x

Input variables that must be monitored in level 2	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Gas pedal [2)]	x	x	x	x
Brake [2)]	x	x	x	x
External requests that increase torque [2)]	x	x	x	x
Air flow (as main load signal)	x	x	-	-
Intake manifold pressure (as main load signal)	x	x	-	-
Fuel mass	-	x	-	-
Engine rotational speed	x	x	x	x
Spark angle	x	x	-	-
Injection triggering duration	-	x	x	x [3)]
Injector triggering variables (e.g. trigger start)	-	-	x	x [3)]
Oxygen sensor	-	x	-	-

[1)] may be required in the future
[2)] „raw signals" at the control unit, see chapter definitions of terms
[3)] at overrun

Function monitoring	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Torque comparison (permissible torque with actual torque)	x	x	x	-
Overrun monitoring	-	-	x	x
Shutoff path test (up to actuator output stage)	x	x	x	x
System reaction (IR) of level 1 in case of error [4)]	x	x	x	x
A/D converter test	x	x	x	x
Plausibility of torque loss from Level 1	x[5)]	x[5)]	x	x
Plausibility of adaption-/ correctionvalues from level 1	x	x	x	x
Cancel cruise control by brake request (internal CC)	x	x	x	x
Acceleration comparison	-	-	-	x

[4)] for error reactions that level 2 cannot convert by itself
[5)] project specific agreement

Reactions in case of error (error-specific)	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Reset	x	x	x	x
Actuator output stage switch-off	x	x	x	x
Replacement operation that reduces the performance (e.g. IR)	x	x	x	x

6.1.3.1 Inclusion torque loss from level 1 for the calculation of “permissible torque”

When using a target torque loss from level 1 to calculate the permissible torque from level 2, this quantity must be verified in level 2. Failure response see appendix.

6.1.3.2 Transfer of adaptation values / correction factors from level 1 to level 2 (tolerance restriction)

If adaptation values and/or correction values with torque effect are transferred from level 1 to level 2, they have to be checked to be in compliance with permissible limits. Failure response see appendix.

6.1.3.3 Monitoring of the injection output variables from level 1

Function: Plausibility of the actual trigger variables in level 2

The measurement variables of the injector triggers available in level 2 have to be checked value specific to be in compliance with plausibility limits.

Examples:

- plausible injection angle ranges
- conformity of maximum number of cylinders
- injection type within maximum injection type number

At impermissible deviations an error in level 1 is to be concluded. Error response see appendix.

6.1.3.4 Monitoring of the trigger output unit (e.g. TPU, PCP)

Function: Comparison of target trigger variables from level 1 with actual trigger variables read back in level 2

For recognition e.g. of toggled or defective RAM cells of the trigger output unit the electrical trigger variables for the injectors read back in level 2 have to be checked to be plausible with the target variables of level 1. Per calculating cycle in level 2 at least one cylinder (e.g. through rotating cylinder pointer) must be checked.

By appropriate measures it must be ensured that impermissible copies of input variables to the output memory get recognized. Error response see appendix.

6.1.3.5 Continuous torque monitoring diesel (torque comparison), determination actual torque level 2

The injection output variables calculated in level 1 are converted into electrical trigger signals by a trigger output unit (e.g. TPU, PCP).

For reverse calculation of the actual torque the electrical trigger signals on the trigger circuits are measured event depending. After transformation into time-, angle- and cylinder depending measurement data they are given as input variables of level 2.

For the further reverse calculation of torque the injection relevant and engine speed synchronous rail pressure is to be used. The requirements for safeguarding this input variable in level 2 are described in the following.

6.1.3.5.1 Rail pressure monitoring

6.1.3.5.1.1 Requirements to level 1

The rail pressure diagnosis must be assigned project specific. For monitoring purposes for single channel rail pressure capturing systems the following minimum scales are to be regarded:

- SRC high / low diagnosis
- rail pressure gradient check (direction specific)

6.1.3.5.1.1.1 Interface signals to level 2

Recognized errors get reported to level 2 via diagnosis status. For protection of the rail pressure in level 2 the variables rail pressure gradient with associating diagnosis status are to be made available in level 2.

6.1.3.5.1.1.2 Backup mode

In case of recognized error it is to be switched to backup mode with rail pressure target value of the rail pressure controller.
For the actual torque reverse calculation in level 2 it similarly is to be switch to this backup variable.

6.1.3.5.1.2 Requirements level 2

In level 2 the raw value of the rail pressure sensor is to be used.

6.1.3.5.1.2.1 Plausibilities

In analogy to level 1 for single channel rail pressure capturing systems the following minimum scales are to be regarded:

- SRC high / low monitoring
- monitoring rail pressure gradient diagnosis of level 1

The monitoring of the rail pressure gradient diagnosis checks if an error is detected in level 1 due to exceeding/ being below a limit value.
In case of error detection the choice of backup mode depends on whether in level 1 a fault has been detected or not (see following description).

6.1.3.5.1.2.2 Backup mode if fault in level 1 detected

For the further reverse calculation of the actual torque in level 2 the rail pressure target value of the rail pressure control is to be used.

6.1.3.5.1.2.3 Backup mode if fault in level 1 not detected

An error exists in level 1. The rail pressure information is not reliably available any more. Error response see appendix.

6.1.3.5.2 Torque relevant efficiencies of injection quantities

If injection quantities get weighted with efficiency factors from level 1 for the determination of torque calculations, these efficiency factors have to be safeguarded in level 2. Error response see appendix.

6.1.3.5.3 Further torque relevant efficiencies (e.g. air influence)

If, inherent to the system, further physical influencing variables leading to further weighting factors for the relevant injection quantities due to the accuracy requirements on the torque to be calculated do exist, the used efficiency factors from level 1 have to be safeguarded in level 2.

6.1.3.6 Continuous monitoring diesel (acceleration comparison)

Alternatively to the “continuous torque monitoring” for diesel, the continuous acceleration monitoring may be realized.

6.1.3.6.1 Requirements level 1

Basic principle:

1. The drivers` input is interpreted as vehicle target acceleration.
2. At overcoming this target acceleration, an acceleration oriented driving behaviour is activated.

Description:

From the target engine torque, the vehicle target acceleration is calculated, using the power train transmission ratio and additional vehicle parameters (e.g. vehicle reference mass, reference c_w-value, etc.) The delivered engine torque is reduced using a controller if the actual vehicle acceleration overcomes the target vehicle acceleration. This controller is to be realized parallel to the torque path and it is limited downwards to 0 Nm (see illustration 5c).
Below an applicable vehicle speed threshold, the acceleration controller is switched to an engine speed controller.

This Function in level 1 serves to ensure the driveability when overcoming the target vehicle acceleration. Thus, an unwanted interference of level 2 (e.g. when driving downhill) is avoided.

6.1.3.6.2 Requirements level 2

In level 2 (illustration 5b), based on redundantly captured input signals, the actual vehicle speed as well as the engine speed is monitored. If the actual vehicle speed for an applicable time is larger than the target acceleration, level 2 limits the driving torque to zero. With it, the overrun monitoring is activated to detect a possible failure (see illustration 4).
Additionally, at an applicable engine speed, the idle run controller and the torque loss compensation is to be deactivated. Thus, it is ensured that the target torque provided by level 1 is certainly 0 Nm.

6.1.3.7 Continuous torque monitoring diesel, overrun monitoring

The overrun monitoring known from present diesel monitoring systems is to be integrated in the continuous torque-/acceleration monitoring as parallel monitoring path for the torque comparison.
Error response see appendix.

6.1.4 Safeguarding of torque output variables in the control unit group

The safeguarding of torque output variables in the control unit group is to be assigned project specific.

6.1.5 Level 3 controller monitoring

Controller monitoring refers to the interaction of the software and hardware structure that enables the function controller hardware diagnostics including but not limited to the controller core, affected areas in RAM/ROM and the clock. In the function controller, the RAM/ROM storage components are normally monitored at least once per driving cycle (initialization or power down). If an error is detected, the check must be executed at the next initialization. Engine start (if software controlled) or combustion is allowed only after the check is completed without errors.

Level 3 consists of 2 basic elements:

- The **physically independent monitoring module** (L3_MM realized through separate hardware) communicates with the L3 monitoring software in the function controller (L3_SW in FC) via an interface. The L3_MM asks one question cyclically to the L3_SW in the function controller FC from at least 10 different questions ; it monitors the receipt of a cyclical test result, makes the assessment and in case of an error initiates the error reaction. To do this, the monitoring module can be either an ASIC or controller.
  When using the RAM/ROM components in L3_MM these components shall be cyclically tested at least once for each driving cycle.

- L3 monitoring software in the function controller (L3_SW in FC) communicates with the L3_MM via an interface. The interaction between L3_MM and L3_SW in FC is also described as question / answer communication.

For this, several test paths shall be worked out in the function controller (see 6.1.4.3).
Each test path gives an accurately defined numerical partial result that depends on the question. The connection of the partial results leads to a numerical total result (test result), that will be transmitted to the L3_MM via the communication interface. The L3_SW in the FC signals the defective operation to the L3_MM by means of correct answers.

Illustration 1 in appendix

6.1.5.1 Monitoring of the question / answer communication

6.1.5.1.1 Monitoring via the L3_MM

The L3_MM expects an accurately determined answer from the L3_SW in the function controller within a given time period. In case of error the L3_MM operates an internal error counter and repeats the wrongly answered question. In the error counter's final state, the monitoring module switches off the performance determining actuator output stages and triggers a SW reset via the function controller. If the L3_MM receives an answer at the wrong moment, the same error reaction is immediately triggered again.The error counter process in the L3_MM must be designed so that error detection states lead to a quicker error reaction threshold than recognized error-free states lead to „an error counter recovery".

The monitoring module must not be subjected to development and modification cycles of a flash control unit and must be independent of the vehicle project or equipment. The questions generated by the monitoring module are generic and determined by the definition of the engine management system. The adjustment to the project-specific characteristics shall be carried out by means of unique parameters on the function controller's side.

6.1.5.1.2 Monitoring via the L3_SW in the function controller

The L3_SW in the FC expects a new question from the L3_MM within a given time period and checks the error-free operation of the L3_MM. The test in the L3_SW in FC is initiated when the L3_SW in FC gives wrong answers at specific time intervals. The next error counter status transmitted in combination with the question from the L3_MM is checked by the L3_SW in the FC to see if the error detection is written in the error counter modification.
In case of error, the L3_SW in FC uses an internal error counter and transmits again a wrong answer to the L3_MM. In the error counter's final state the function controller switches off the actuator output stages and triggers an unlimited number of resets to increase the availability.

Illustration 1 in appendix

6.1.5.2 Iteration rate of the question / answer communication

The iteration rate must not exceed a limit value of 80 ms. This is required to guarantee sufficient quantification for the error handling.

6.1.5.3 Test paths of the L3_SW in the function controller

Independent test paths that build a partial answer each time for the L3_MM must be differentiated:

- Program flow check

The program flow check verifies that all level 2 program modules (including TPU, cyclic RAM/ROM tests) that are relevant for monitoring, are processed in fixed timeslot patterns and with the right sequence.

- Function-specific instruction set test

It enables the detection of errors in the controller core and execution of level 2 functions and must be adapted to the safeguarding relevant monitoring functions.
To avoid disturbing the level 2 sequences, a copy of the safeguarding relevant ranges is filed in a specific RAM and ROM area. With these, the level 2 test questions are representatively answered. All selected test data represents fictitious level 1 error states and generates an appropriate part of answer. The functionality of all safeguarding relevant controller instructions of the copied volumes shall be tested.

6.1.5.4 Question generation in monitoring module L3_MM

The amount of questions and the quality of the corresponding input data sets for the function-specific instruction set test must be defined to provide comprehensive error detection (10 questions at least).

The monitoring module L3_MM selects a pre-determined set of different questions that are submitted to the function controller.

As a consequence of pseudo random results, the interval between similar questions is reduced (which means no pure random sequence). Through this, processing time for all determined questions is also limited.

6.1.5.5 TPU monitoring

The TPU´s or comparable hardware components are capable of operating independently. This can have an influence on the safety-relevant signals and they must be included in the monitoring concept for the function controller.

The aim of monitoring is to discover the following errors:

- Destroyed cells in the internal parameter memory
- Data flow conflicts for systems that use shared storage areas
- Non-plausibility in TPU calculation variables

The monitoring characteristics are:

- Writing properties test of the parameter memory (for ex. TPU- internal parameter RAM)
- Program memory storage test (for ex. TPU program RAM cyclically, ROM once per driving cycle)
- TPU monitoring is included in program flow checking.
- Plausibility of TPU characteristic calculation variables in the function controller (for ex. plausibility of the speed calculation in the TPU by assessing separate segment interrupt times)

Error reaction

- In case of error, a reset is triggered in the function controller.

6.1.5.6 Shutoff path test

Monitoring purpose

- Check the shutoff paths to the performance determining output stages, so that a safe shutoff is guaranteed in case of error.

Monitoring characteristics

- One test per driving cycle
  Remark : if the test is carried out during power down and no positive results were obtained, a new test must be carried out during the next initialization phase.

- Engine run is authorized only after one successful shutoff path test per controller.

Error reaction

- Reset until engine run authorization
  (see also 6.1.4.8 System behavior at reset)

6.1.5.7 A/D conversion test

The purpose of the A/D conversion test is to cover three different error possibilities:

The following table shows a procedure to recognize A/D conversion errors that could occur depending on the present system:

Error possibility	ID – Test pulse procedure PTS 2 inputs	Reference voltage of a free ADC channel	2 ind. A/D converter in the system
Gain error		x	x
offset error	x		x
Stuck regis-ters (MUX does not operate either)	x		x

6.1.5.8 System behavior at reset

Effect:

- The reset affects the monitoring module (MM) and the function controller (FC)
- The performance determining output stages are switched-off
- The duration of the reset status must be determined specifically for the project

Tests after reset:

- The stored information regarding the cause of the SW reset is assessed before the next engine start can be authorized. In the case of a recognized RAM/ROM error, check the whole level 2 storage area before a new release occurs. Unless required otherwise, the remaining RAM/ROM areas shall be checked during the driving cycle.
- The maximum authorized number of SW resets in one driving cycle shall be determined according to the project. Subsequently, the performance determining output stages are to remain de-energized until the driver restarts.

Restart after reset:

- The MM is synchronized with the FC over the determined question / answer communication sequence. Thus, adjustment and test actions are related to test the MM and FC shutoff path. The test gives a statement of the operating capability of both shutoff paths.
- The performance determining output stages are released after successful test.

Illustration 6 in appendix

6.1.5.9 Diagram of the level 3 error reactions

Illustration 6 in appendix and Illustration 7 in appendix

6.2 System reactions in case of error

The following principles are valid when considering the error reactions :

- The necessary plausibility tolerances depend on the vehicle's manufacturer and the project.
- If limp-home air driving is required and limp-home position is not reached, IR will be activated (gasoline).
- The maximum error detection duration up to beginning of the system reaction shall be determined according to the error (e.g. directional duration of 500 ms during torque monitoring)
- The detection of definite errors in level 2 leads to activation of IR directly or indirectly by the torque comparison or acceleration comparison (gasoline / diesel).

See detailed table of the error reactions in appendix.

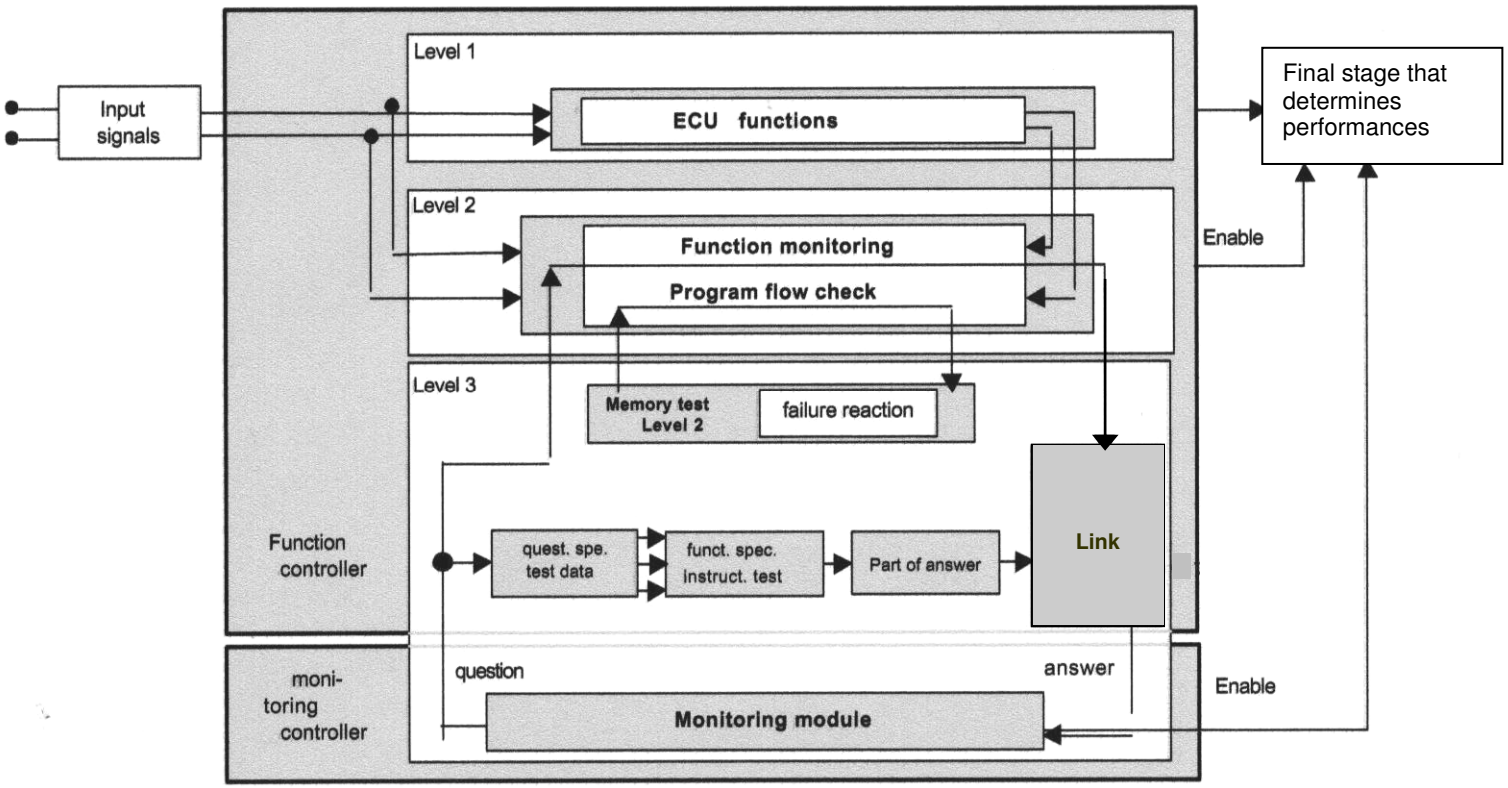
6.3 Additional technical requirements

6.3.1 Safe engine stop

Stop the combustion engine with ignition off. Use a shutoff path in the control unit, which is independent from the (main) controller and by suitable procedures (e.g. intervention in ignition, fueling device or injectors for fuel injection, fuel pump etc.), to guarantee the combustion engine is stopped redundantly with permissible time delay when recognizing ignition off.
Other comparable executions are to be agreed with the OEM.

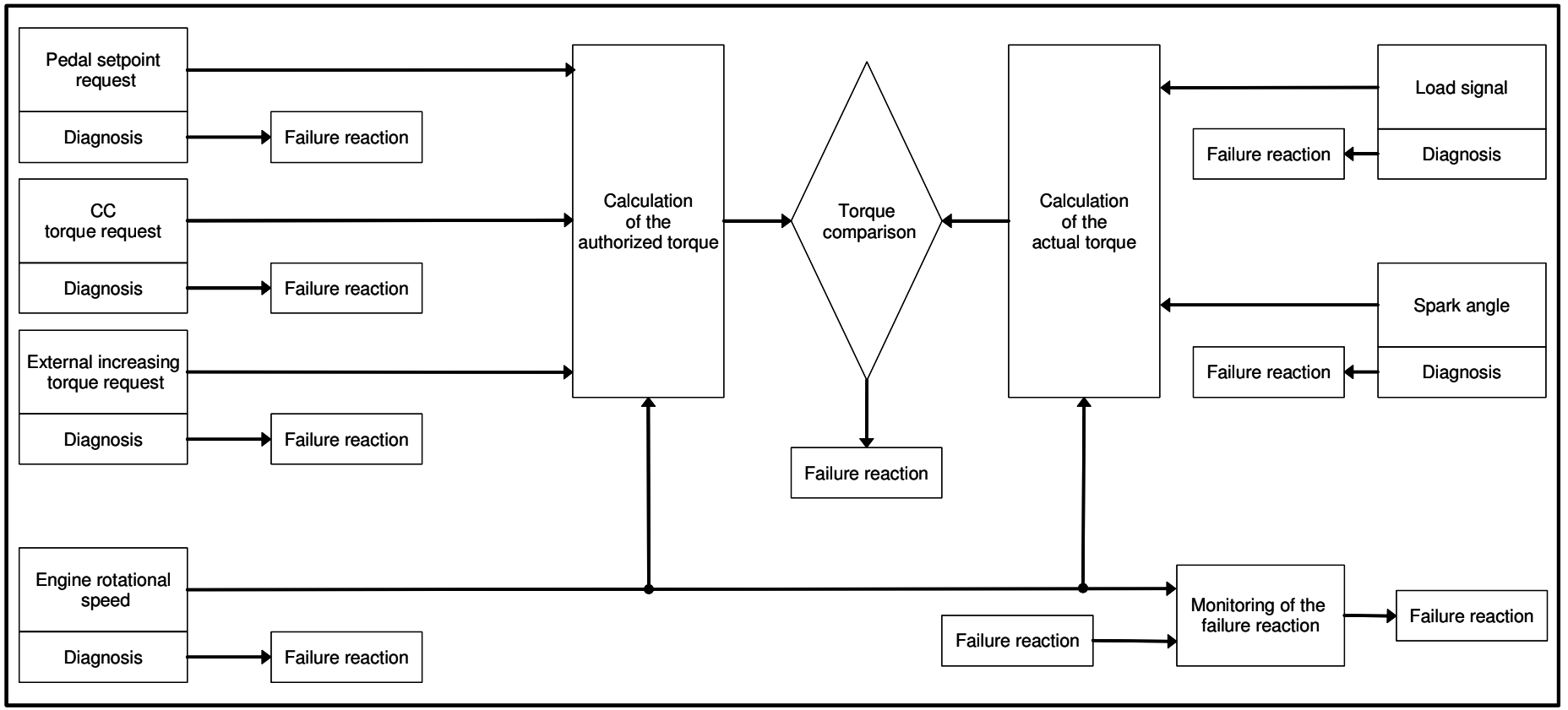
7 7 APPENDIX: ILLUSTRATIONS

Illustration 1: System overview



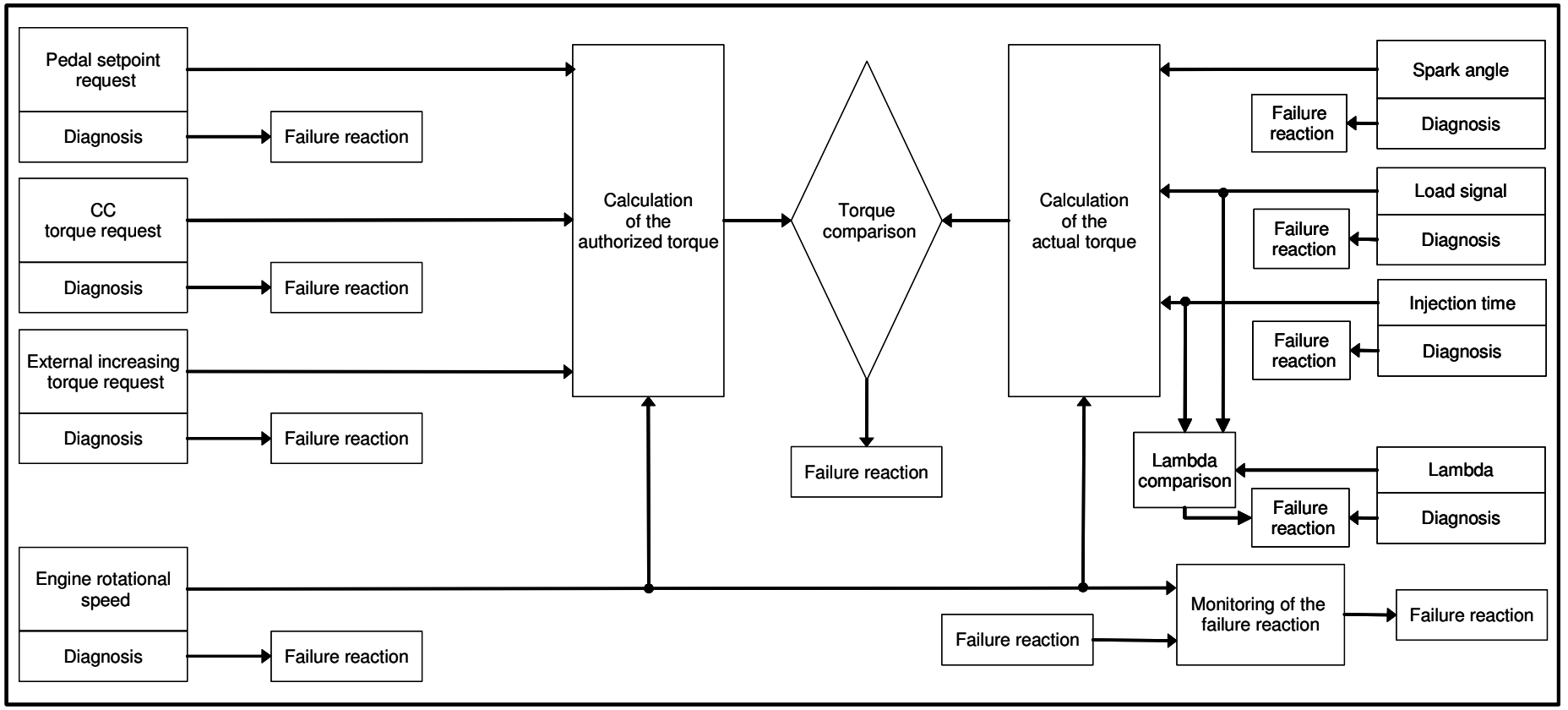
Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS work group

Illustration 2: Level 2 function monitoring, gasoline manifold injection



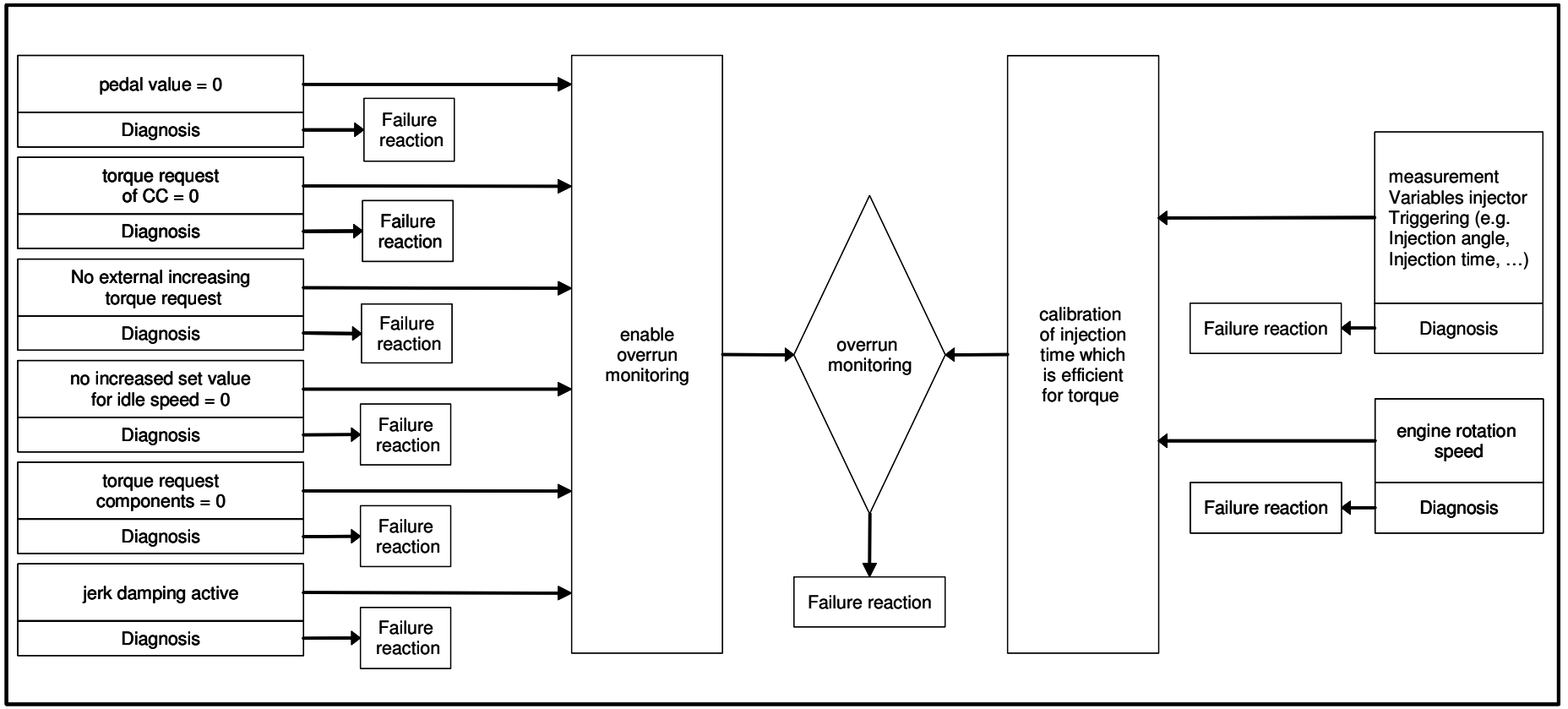
Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS work group

Illustration 3: Level 2 function monitoring, gasoline direct-injection engine



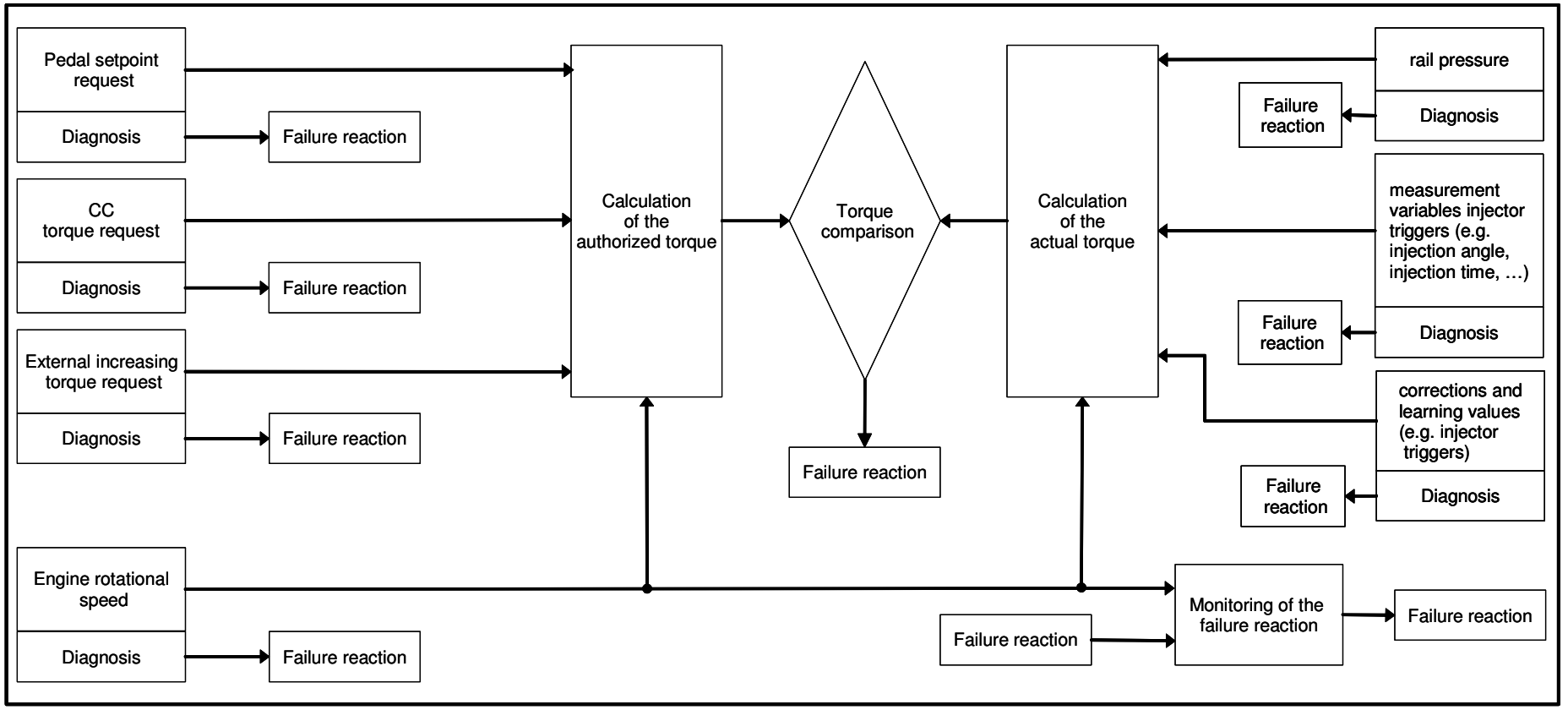
Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS work group

Illustration 4: Level 2 function monitoring, diesel / continuous torque monitoring (overrun monitoring)



Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS work group

Illustration 5a: Function monitoring level 2, diesel / continuous torque monitoring (torque comparison)



Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS work group

Illustration 5b: Function monitoring level 2, diesel / continuous torque monitoring (acceleration comparison)

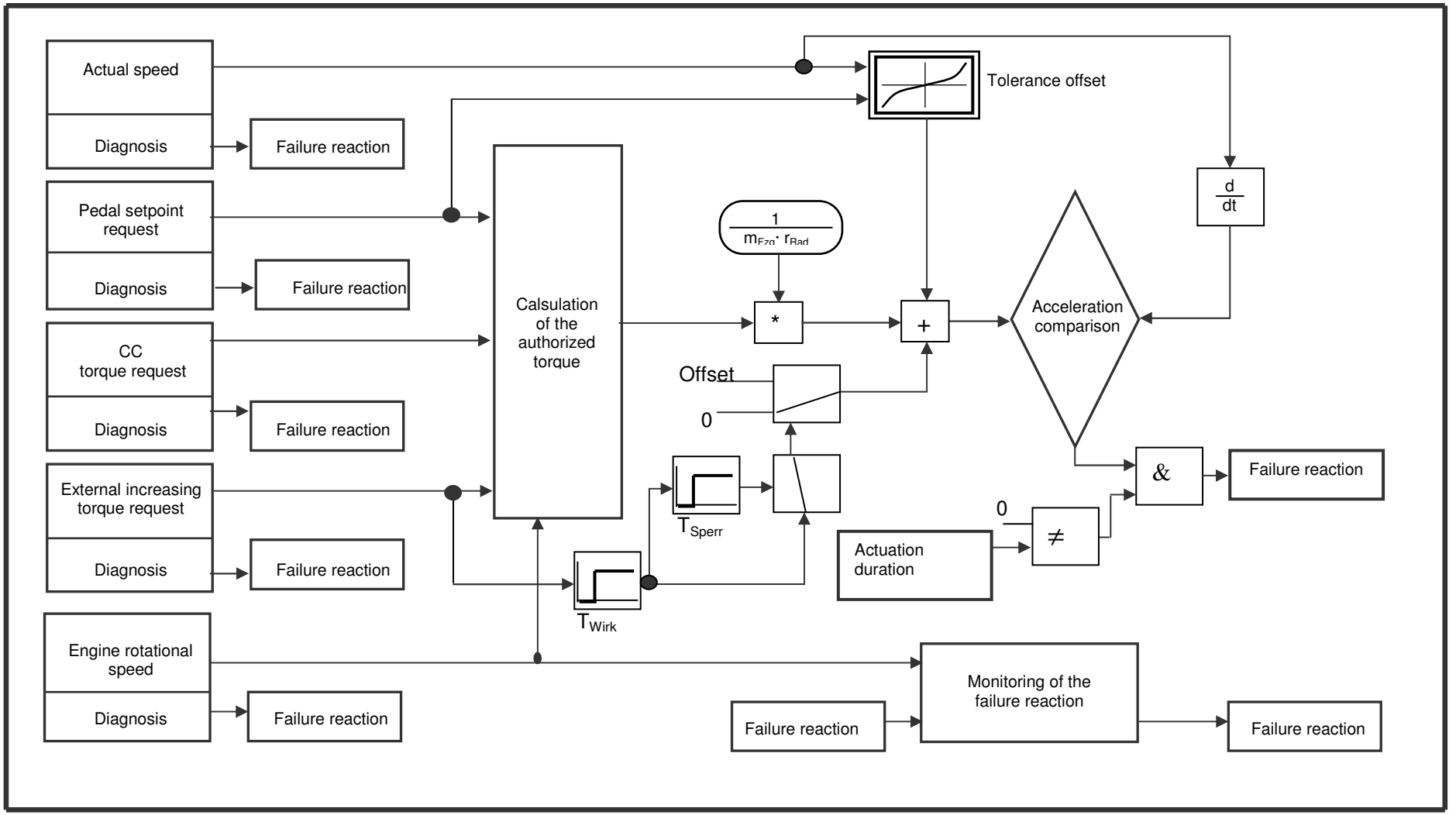


Illustration 5c: Diesel / continuous monitoring (acceleration comparison), overview

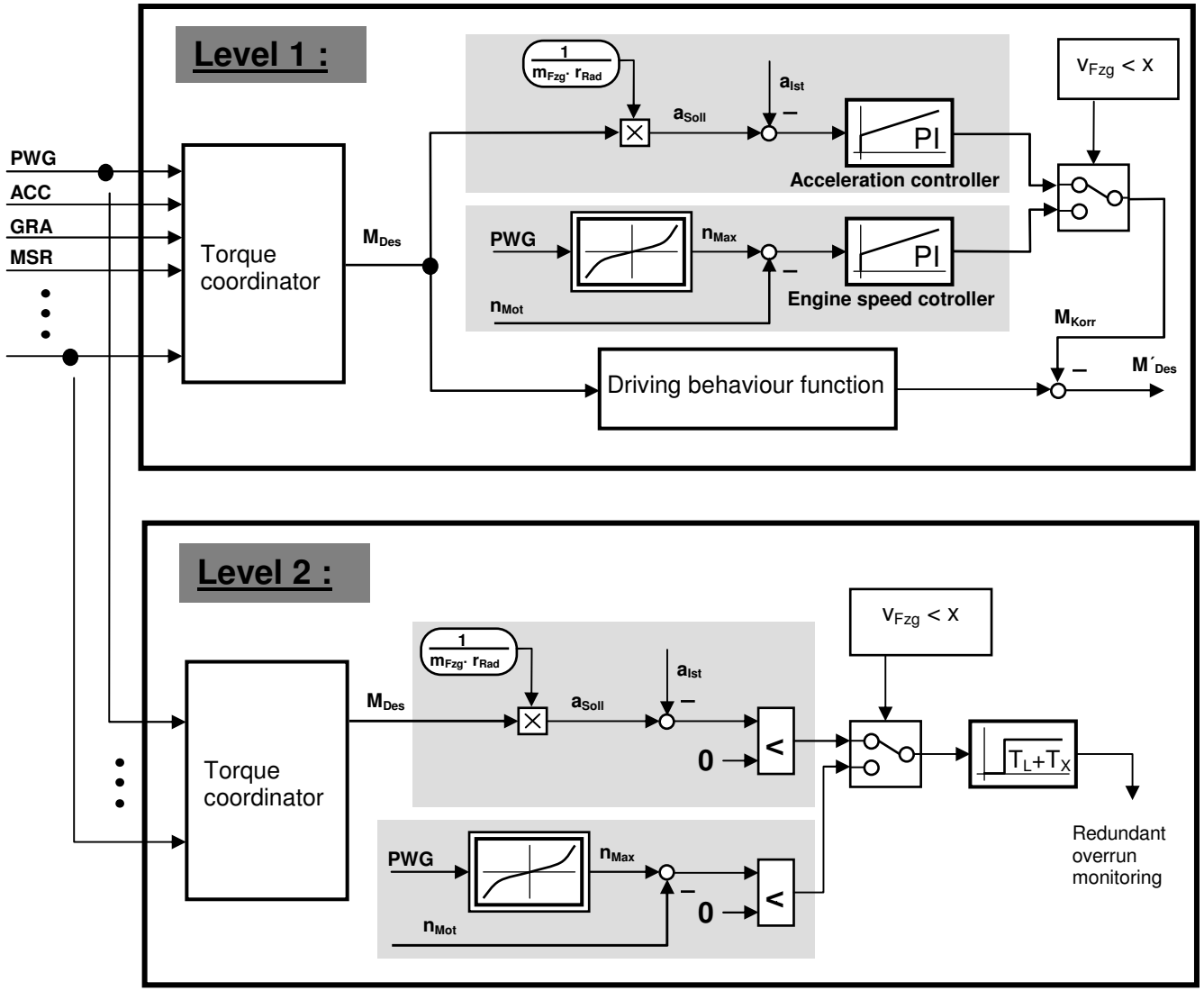
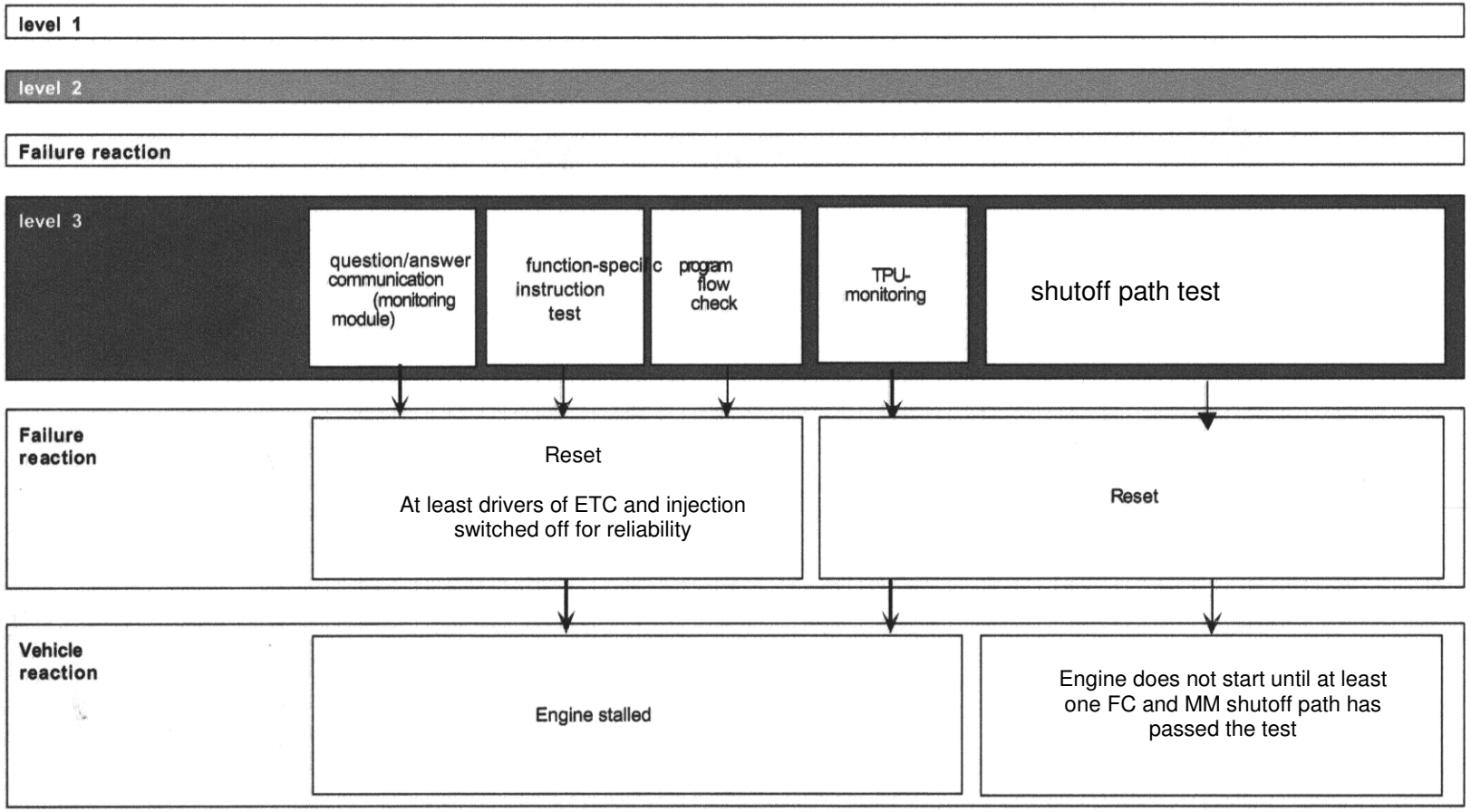
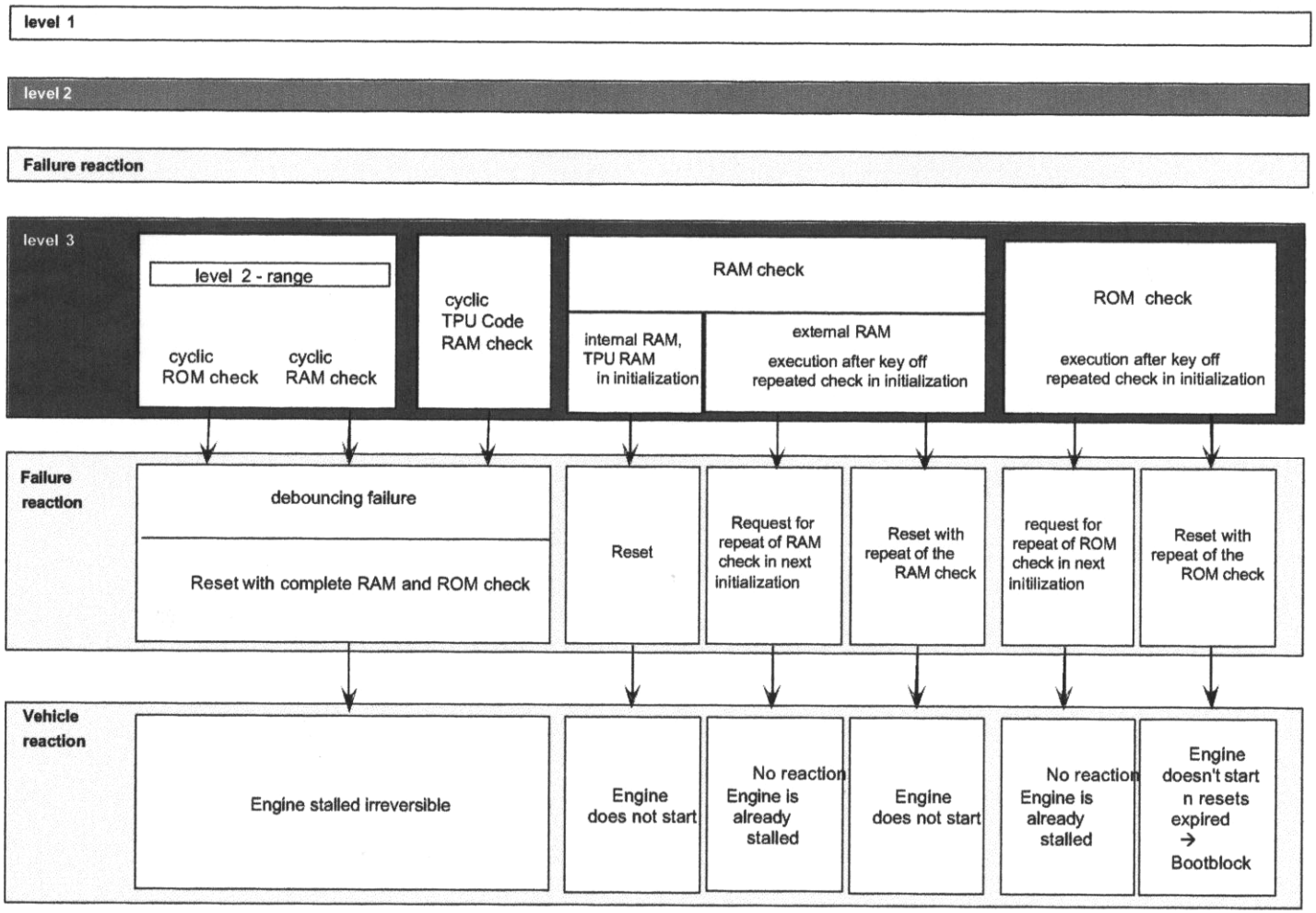


Illustration 6: Level 3 controller monitoring failure reactions, gasoline and diesel



Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS work group

Illustration 7: Level 3 memory test failure reactions: gasoline and diesel


level 1
level 2
Failure reaction
level 3
level 2 - range
cyclic ROM check
cyclic RAM check
cyclic TPU Code RAM check
RAM check
internal RAM, TPU RAM in initialization
external RAM
execution after key off
repeated check in initialization
ROM check
execution after key off
repeated check in initialization
Failure reaction
debouncing failure
Reset with complete RAM and ROM check
Reset
Request for repeat of RAM check in next initialization
Reset with repeat of the RAM check
request for repeat of ROM check in next initilization
Reset with repeat of the ROM check
Vehicle reaction
Engine stalled irreversible
Engine does not start
No reaction Engine is already stalled
Engine does not start
No reaction Engine is already stalled
Engine doesn't start n resets expired → Bootblock

Basic concept of the Robert Bosch GmbH. Extent or modification via the EGAS work group

8 APPENDIX : FAILURE REACTIONS

8.1 Error from the level 1 monitoring

8.1.1 Pedal-travel sensor

Error	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel
target value 1 > threshold (signal-range-check high)	Back up mode target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification
target value 1 < threshold (signal-range-check low)	Back up mode target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification
target value 2 > threshold (signal-range-check high)	Back up mode target value 1 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 1 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 1 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification
target value 2 < threshold (signal-range-check low)	Back up mode target value 1 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 1 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode target value 1 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification
Non-plausibility between target value 1 and target value 2 Target value 1 - target value 2 > threshold	Back up mode with min. from target value 1 and target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode with min. from target value 1 and target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification	Back up mode with min. from target value 1 and target value 2 with max. value and max. gradient limitation. Brake actuated / brake signal error = idle speed specification
Supply voltage PTS outside the authorized areas (system with a power supply line)	Idle speed specification	Idle speed specification	Idle speed specification
Back up mode with target value 1 and target value 1 > threshold (signal-range-check high)	Idle speed specification	Idle speed specification	Idle speed specification
Back up mode with target value 2 and target value 2 > threshold (signal-range-check high)	Idle speed specification	Idle speed specification	Idle speed specification
Back up mode with target value 1 and target value 1 < threshold (signal-range-check low)	Idle speed specification	Idle speed specification	Idle speed specification
Back up mode with target value 2 and target value 2 < threshold (signal-range-check low)	Idle speed specification	Idle speed specification	Idle speed specification

8.1.2 Throttle actuator (gasoline with one throttle-valve actuator)

DLW (throttle valve replacement value) designed according to project (for example : from air flow / intake manifold pressure, engine rotational speed)

Error	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine
TV 1 > threshold (signal-range-check high)	Back up mode with TV2 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)	Back up mode with TV2 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)
TV 1 < threshold (signal-range-check low)	Back up mode with TV2 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)	Back up mode with TV2 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)
TV 2 > threshold (signal-range-check high)	Back up mode with TV1 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)	Back up mode with TV1 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)
TV 2 < threshold (signal-range-check low)	Back up mode with TV1 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)	Back up mode with TV1 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)
TV1 - TV2 > threshold TV2 plausible / TVDV	Back up mode with TV2 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)	Back up mode with TV2 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)
TV1 - TV2 > threshold TV1 and TV2 non-plausible / TVDV	Irreversible IR of level 1 TV without current	Irreversible IR of level 1 TV without current
TV1 - TV2 > threshold TV1 plausible / TVDV	Back up mode with TV1 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)	Back up mode with TV1 and comparison with TVDV - the TV opening is limited as a function of the engine speed (nist)
Back up mode with TV1 and plausibility with TVDV and TV1 < threshold or TV1 > threshold	Irreversible IR of level 1 TV without current	Irreversible IR of level 1 TV without current
Back up mode with TV2 and plausibility with TVDV and TV2 < threshold or TV2 > threshold	Irreversible IR of level 1 TV without current	Irreversible IR of level 1 TV without current
Back up mode with TV1 and plausibility with TVDV is active ; a load sensor error occurs	Irreversible IR of level 1 TV without current	Irreversible IR of level 1 TV without current
Governor error target / current value comparison	Irreversible IR of level 1 TV without current	Irreversible IR of level 1 TV without current
Governor error Input variable	Irreversible IR of level 1 TV without current	Irreversible IR of level 1 TV without current
Final stage error	Irreversible IR of level 1 TV without current	Irreversible IR of level 1 TV without current

8.1.3 Monitoring of external requests

Error	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel
Defective / missing message for external torque requirements (detection in level 1)	The requirement is blocked customer-specific reversible or irreversible Customer-specific torque transition function	The requirement is blocked customer-specific reversible or irreversible Customer-specific torque transition function	The requirement is blocked customer-specific reversible or irreversible Customer-specific torque transition function

8.1.4 Monitoring programming and supply voltage

Error	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel
Flash : programming not ended	Remains in boot block	Remains in boot block	Remains in boot block
Flash : programming error	Remains in boot block	Remains in boot block	Remains in boot block
Supply voltage outside specification	Reset	Reset	Reset

8.1.5 Brake information

Error	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel
Non-plausibility of the redundant brake signal	Switch off CC	Switch off CC	Switch off CC

8.2 Failure from the level 2 functional monitoring

Error	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel torque comparison	Diesel acceleration comparison
Defective / missing message for external torque increasing requirements (MSR, transmission, etc.) (detection in level 2)	Reaction analog to "defective / missing message for external torque requirements (detection in level 1)"	Reaction analog to "defective / missing message for external torque requirements (detection in level 1)"	Reaction analog to "defective / missing message for external torque requirements (detection in level 1)"	Reaction analog to "defective / missing message for external torque requirements (detection in level 1)"
Defective engine speed : deviation between level 1 and level 2 (detection in level 2)	Reset	Reset	Reset	Reset
Defective driver's demand detection : deviation between level 1 and level 2. (detection in level 2)	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2
Cancel error or non-authorized activation of the cruise control (detection in level 2)	Deactivate CC request : if locking not possible : require / monitor respond torque comparison, irreversible IR from L2, TV without current	Deactivate CC request : if locking not possible : require / monitor respond torque comparison, irreversible IR from L2, TV without current	Deactivate CC request : if locking not possible : require / monitor respond torque comparison, irreversible IR from L2	Deactivate CC request : if locking not possible : require / monitor respond torque comparison, irreversible IR from L2
Defective fuel mass, oxygen sensor, load signal (detection in level 2)	-	Plausibility in level 2 only in single layer mode ; irreversible locking of the single layer mode, transition to homogenous operation	-	-
Inappropriate injection triggering duration (detection in level 2)	-	Transition to homogenous operation	See below	-

Defective spark angle (detection in level 2)	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	-	-
Plausibility error of the load signal with the throttle valve angle (detection in level 2)	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	-	-
Continuous torque / overrun monitoring: Non-authorized injector triggering due to error in level 1 during overrun fuel cut-off with driver idle speed request (detection in level 2)	-	-	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2
Continuous torque / overrun monitoring: Non-authorized engine torque upper deviation due to error in level 1 (detection in level 2)	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	-
IR is not applied in level 1 (detection in level 2)	Reset	Reset	Reset	Reset
A/D converter error	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2
Error at torque loss from level 1 (detection in level 2)	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2 (only necessary at adequate compen-sation in level 1)
Plausibility error of the actual trigger variables in level 2 (detection in level 2)	-	-	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2
Monitoring error of the trigger output unit (TPU, PCP etc.) (detection in level 2)	-	-	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2
Error at rail pressure monitoring (detection in level 2)	-	-	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	-

Error at the assumption of adaption values / correction factors from level 1 to level (tolerance restriction); Failure in path reverse calculation of actual torque	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2	-
Error at the assumption of adaption values / correction factors from level 1 to level (tolerance restriction); Failure in path calculation of permissible torque	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current; resp. project specific error response	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2, TV without current; resp. project specific error response	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2; resp. project specific error response	After an applicable number of resets and no error suppression, require / monitor irreversible IR from L2; resp. project specific error response (only necessary at adequate compen-sation in level 1)
Error at the assumption of torque relevant efficiencies for injected fuel quantities from level 1 (detection in level 2)	-	-	Demand on L1: Change to an operating mode without relevant efficiency	-
Continuous acceleration monitoring: Non-authorized acceleration upper deviation due to error in level 1	-	-	-	Require / monitor irreversible IR from L2
Acceleration- / v-signal captured incorrect	-	-	-	Switch to substitution v-signal from engine speed

8.3 Failure from the level 3 controller monitoring

Error	Gasoline mult. fuel inj. engine	Gasoline direct inj. engine	Diesel
Wrong time / error counter message in the question / response program (detection via FC)	Reset	Reset	Reset
Wrong response / time in the question / response program (detection via MM)	Reset	Reset	Reset
Error in the shutoff path test	Reset until engine operation is authorized	Reset until engine operation is authorized	Reset until engine operation is authorized
Error in the non-volatile memory	Reset	Reset	Reset
Error in the volatile memory	Reset	Reset	Reset
Error TPU monitoring	Reset	Reset	Reset